ABSTRACT

Method and apparatus for providing secure, controlled access to one or more functions in an electronic system which may have a plurality of functions having different access requirements. A desired function is enabled according to the result of a first authentication process which uses a public key which corresponds to the desired function, and access to the function is authorized by a second authentication process which uses a second, private session key computed as a result of a random challenge made by the system to an external entity during the first authentication process. Additional protection is also provided against passive and active wiretapper attacks, such that only an entity that has received authorization can access the system at the correct access level.